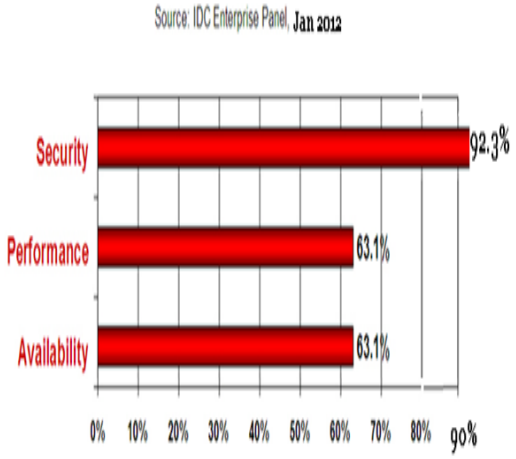
IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013
ISSN: 2320 - 8791
www.ijreat.org

Fault Tolerant Design Approach & Performance Measure for Data Security in Cloud

[1]Snehal Wasankar, [2]Dr.P.R.Deshmukh
[1]ME(II), Sipna C.O.E.T, Amravathi
[2]Sipna C.O.E.T,Amravati

Abstract: Cloud is one of the fastest growing segment of IT enterprises ,I design fault tolerant approach for Data security in cloud Infrastructure .In this implementation part I have design own cloud ,when user want to access the cloud first user should activate the account by using payment, direct user entry in not allowed ,as on cloud user send desired documents ,files, or Access from it ,then users' documents is there for modification point of view. Cryptography tool have designed for Static Data security & RSA is used for Dynamic Data Security, So for that design the cloud Coordinator, Cloud Exchange ,Datacenters.



Practical Implementation

As working cloud is Private ,our own cloud ,developing a data centers on which we form one cluster ,all data center have a replication of data,& Checking each data center for data security, it provides the security in terms of

1.Access Control
2.Identification & Authorization
3.Configaration Managing Control
4.Audit & Standard Algorithms
5.Data mantainance
6.Personal User Security

Security includes

a. Communication Security
b. Protecting Resources from unauthorized data
c. Maintaining performance

IDC provides survey report to understand IT cloud Security.
In this first part is

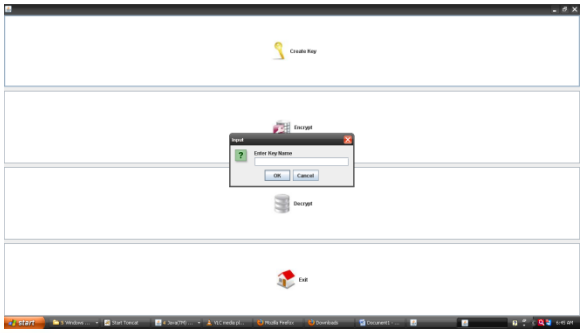
a. User interfacing
b. Implantation of Practical execution environment

Design Parameters

a. Cloud Coordinator
b. Cloud Exchange Manager
c. Datacenters for storage
d. Data Broker

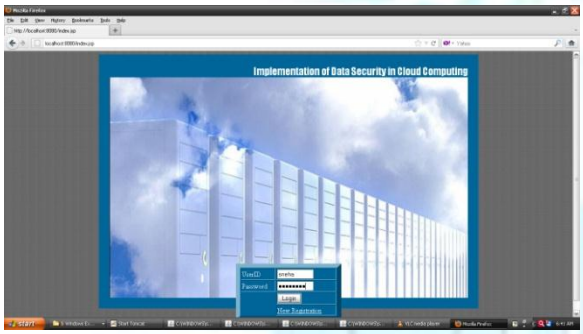
1.Working of Cloud Coordinator
a.in IAAS,PAAS Export Cloud Services
b. Adjust load on cloud resources
c.cloud coordinator have a private key for deciphering user data. All datacenters have a replica of Data.it monitors the classes like
1.ccserver
2.Filemanager

3.Storage Manager
4.Crypto RSA
5.Crypto Class for AES-Static data
6.Checksum ,Checking of data with MD5
7.UDPFILE SEND
8.UDPFILE RECIVE
9.DCFILE SEND
10.DCFILE STORE

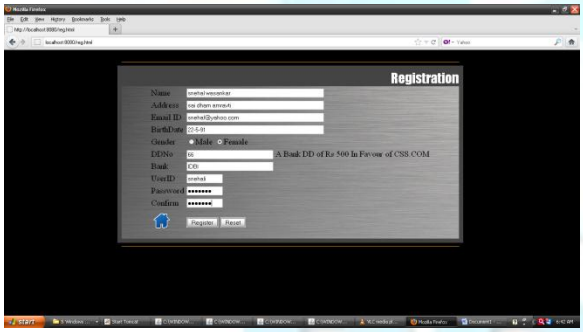


Result/Implementation

1.UserAuthentication



2.Activationuser



3.Working Area of cloud

4.Cryptography

Implementation of Data Centers

Servers on cloud,Each data centers with unique port number & IP address all data centers they are in cloud,All data centers are wait at particular port number,this is for storage point of view,that provides IAAy S hardware service it associates withmemeory ,capcity,storage.

Implemntation of Data Broker

This class maximize the perfomance of data centers,intermidiator between user & cloud coordinator,cloud exchange.

Crypto Class

The methods in the Crypto class provide standard algorithms for creating digests, message authentication codes, and signatures, as well as encrypting and decrypting information. These can be used for securing content in Force.com, or for integrating with external services such as Google or Amazon WebServices (AWS).

Decrypts :the blob *cipherText* using the specified algorithm, private key, and initialization vector. Use this method to decrypt blobs encrypted using a third party application or the encrypt method.

Valid values for *algorithmName* are:

- AES128
- AES192
- AES256

These are all industry standard Advanced Encryption Standard (AES) algorithms with different size keys. They use cipher block chaining (CBC) and PKCS5 padding.The length of *privateKey* must match the specified algorithm: 128 bits, 192 bits, or 256 bits, which is 16, 24, or 32 bytes, respectively. You can use a third-party application or the generateAesKey method to generate this key for you.The initialization vector must be 128 bits (16 bytes.)

Encrypts: the blob *clearText* using the specified algorithm, private key and initialization vector. Use this method when you want to specify your own initialization vector. The initialization vector must be 128 bits (16 bytes.) Use either a third-party application or the `decrypt` method to decrypt blobs encrypted using this method. Use the `encryptWithManagedIV` method if you want Salesforce to generate the initialization vector for you. It is stored as the first 128 bits (16 bytes) of the encrypted blob.

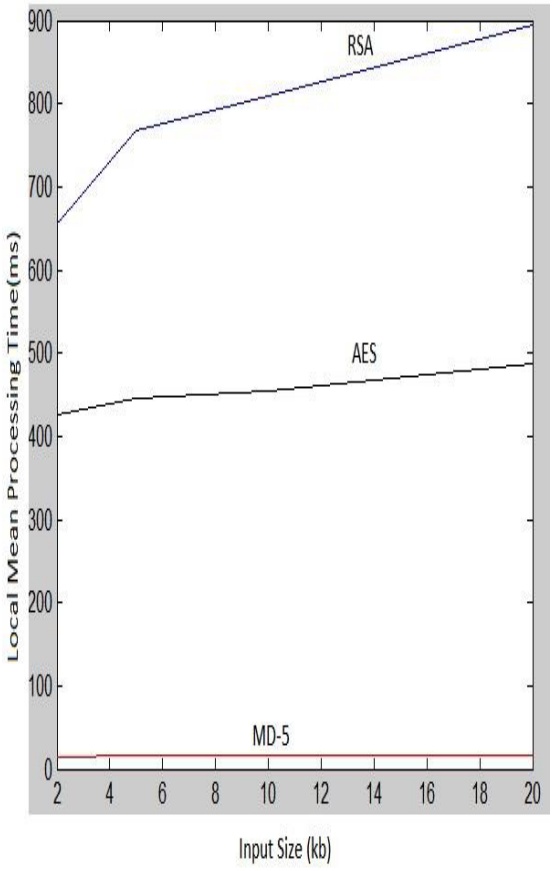
Valid values for algorithmName are:

- AES128
- AES192
- AES256

These are all industry standard Advanced Encryption Standard (AES) algorithms with different size keys. They use cipher block chaining (CBC) and PKCS5 padding.

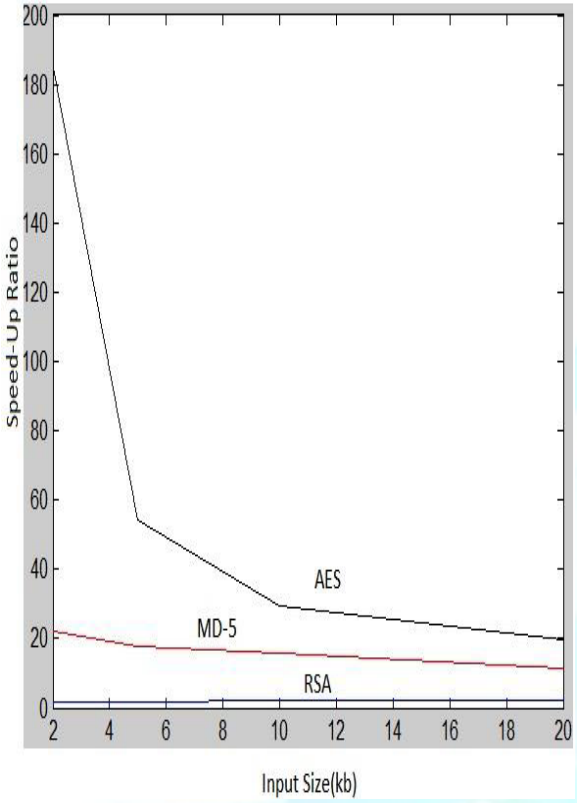
The length of *privateKey* must match the specified algorithm: 128 bits, 192 bits, or 256 bits, which is 16, 24, or 32 bytes, respectively. You can use a third-party application or the generateAesKey method to generate this key for you.

Comparisan Results



Measuring perfomance in terms of

1. Time required for file send
2. Time required for file recive
3. Tme for Encryption RSA
4. Time for decryption AES
5. Size of file
6. Security measure
7. Efficiency



Conclusion

Cluster creation in data centers prevent Data loss,when all datcenters were broken then all data will retrive from Admin,Perfomance analyasis shows that the proposed scheme highly efficient & resilient against maliciaous data modification attack,Fault tolerant,So data is secured in cloud(Private cloud)

Referances

[1] Priyanka Arora, Arun Singh World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012 179

[2]Shamir, A:How to share a Secret,Comm of the ACM 22,612-613(1979)

[3]Popvi kresimir, hocenski Zeljkoo(2010).”Cloud computing security issue and challenges”In Proceeding of 33 rd International Convention, IEEE transaction(PP.344-349)

[4]Eric A.Marks Bob Lozano(2010)”Executive guide to cloud computing”http://www.execsguidetocloud.com/(sept.5,2010)

[5] G. Jai Arul Jose1, C. Sajeev2, Dr. C. Suyambulingon Research Scholar, Sathyabama University, Chennai, INDIA Tamil Nadu Agricultural University, Coimbatore, INDIA” Implementation of Data Security in Cloud Computing” International Journal of P2P Network Trends and Technology- Volume1Issue1-2011 ISSN: 2249-2615 http://www.internationaljournalssrg.org